Remarks

As an initial matter, the Examiner's indication that claim 52 includes allowable subject matter is appreciated. Claim 52 has been amended to independent form and is believed to be in condition for allowance. Claims 2, 54-58 and 70-72 have been canceled.

Objections

The Examiner objected to the drawings as failing to specifically included the "second information" of claim 73. The specification has been amended to refer to FIG. 14, and the Examiner's approval of the corresponding addition to FIG. 14 (shown in red on the attached drawing sheet) is respectfully requested.

Withdrawal of the objection is requested.

Rejections under 35 U.S.C. §112

Claims 65-69 have been rejected under 35 U.S.C. §112, second paragraph, as being indefinite. Claim 65 has been amended to render the rejection moot, and withdrawal of the rejection is requested.

Rejections under 35 U.S.C. §102

Claims 1, 3-17, 25-51, 61-63, 65-69, 73 and 74 have been rejected under 35 U.S.C. §102(e) as being anticipated by U.S. Patent No. 5,754,654 to Hiroya et al. ("Hiroya"), and/or U.S. Patent No. 5,898,154 to Rosen ("Rosen") or U.S. Patent No. 5,297,026 to Hoffman ("Hoffman").

In claim 1, a single issuer's signature signs both the first information, e.g. the bearer public key, and the second information representative of a commodity, e.g. a monetary value. Because both the bearer public key and the monetary value are signed with a single signature, the two elements are tied together. As such the issuer's public key endorses the coupling of the monetary value to the bearer public key.

In contrast, although Hiroya does consider signing ticket information data 610 (see Hiroya, column 15, lines 38-40, e.g.) and a local public key PT1i with secret keys STk and STg, respectively, Hiroya does not appear to propose signing both the ticket information data 610 and the local public key PT1i with *both* the same key and the same signature. Consequently, a forger could mix and match signatures of the ticket

information data 610 and the local public keys PT1i, as the two pieces of information are not tied together by any one signature.

Tying the two pieces of information together in the manner provided by the claimed invention allows the bearer to independently verify that the money remains valid. Hiroya's system, however, would allow the issuer to discredit the money as already being spent if a duplicate copy is presented, since it is not cryptographically bound by the bearer's public key. Instead, Hiroya would allow a monetary value to be transferred to another user and spent using an alternative public key. Since in Hiroya's system the issuer has all of the information concerning the ticket, the issuer could send it out again, spend it, then claim it was spent when the original ticket bearer presented his ticket for payment. In this manner, the Hiroya system does not provide proof of a promise to pay the bearer, as is the case with a physical paper money or a check, for example.

With regard to the passages cited by the Examiner, it is respectfully submitted that Hiroya clearly indicates that the public key Li is signed by one signature, the global secret key Sg (see Hiroya, column 14, lines 5-6, for example), and the message R is signed by another signature, the secret local key of the receiver, SLr (see Hiroya, column 14, lines 10-15, for example). Hiroya also signs the secret public key PLs with the global secret key Sg and separately signs the message VR with the signature Sls, the secret local key of the sender. No indication has been found that Hiroya's ticket information data 610 includes any public key information. In addition, Hiroya retains PT1i signed by STk, but does not sign a monetary value. The message R also does not contain any public key information, and PT1i lacks monetary information.

With regard to claims 13, 14 and 36, Hiroya signs a local public key and the message with different secret keys. No disclosure has been found for signing both the message and the public key with a single signature. Furthermore, no disclosure has been found in Hiroya of the "third information" STk (secret key) signing the public key PT1i as suggested in the Office Action.

With regard to claim 25, the transaction number does not link to the applicant's identification in Hiroya, since anyone else could present a transaction number. Only the applicant knows the secret key for applicant's identification. Consequently, the present invention also provides an improved mechanism for presenting a note for payment without revealing the bearer's identification.

In Hiroya, if a different public key PT12 is used to redeem the ticket than the public key used to purchase it, the issuer could falsely claim the money had been spent

and if the purse and the bank records do not reconcile, there is no proof where the error lies. Conversely, in the method provided by the present invention, the bearer's note shows which public key must be used to redeem the note and this key is signed by the issuer.

Hiroya assumes the transaction history cannot be tampered with, and the issuer cannot mark tickets as spent, or the bearer mark them as unspent. The present invention provides a method that prevents the issuer from marking as spent notes without a bearer public key and the bearer from marking them as unspent once a bearer public key signature is sent to the bank with redemption instructions.

The present invention also provides a method whereby a counter signature corresponds to the bearer public key rather than the publisher's or issuer's public key.

With regard to the Rosen reference, Rosen discloses an electronic ticket storage device that is retained by the purchaser and can be connected to a network for transmission and reception of data between vending and refunding devices and the storage device for the execution of electronic money transactions and an electronic ticket which is electronically signed. In Rosen, the bank signs first the money at the money generator module before it sends the note to the bearer. As the note is passed from bearer to bearer, it does not return to the bank but collects a transaction history, all of which is unsigned by the bank. The note does not contain the bearer's signature signed by the bank.

In claims 1, 13, 15 and 63, the bearer's public key information is not the same as the identifier for the money generator module since the keys for the money generator module are controlled by the bank, not the bearer. (See Rosen, col. 7, lines 30-45 and col. 22, lines 41-47, e.g.)

With regard to claims 5-7, in Rosen the list of transfer records lists the identification number of the receiver, not the public key of the receiver. This public key is linked to the identification number only by the certificate provided by the certification authority (see Rosen, column 22, lines 44-47). As such, the note's validity depends on both the bank and the certification authority.

In such an arrangement, a dishonest certification authority could provide his own certificate corresponding to a note bearer's identity and with this and a duplicate of the note he could spend that note without the bearer's public key. Additionally, by refusing to recertify the bearer, the certification authority could prevent the bearer from using his own note. As such, the note is not a proof of a contract of debt between the bank and the bearer only, but requires the good faith of the issuing authority. This differs from the

system provided by the present invention that maintains the note as a single stand-alone proof of promise to pay the bearer, dependent on no other parties for validation.

With regard to claims 18-26, in the claimed invention a bearer is sure that his value notes are valid even if the tamper resistance of the device storing the value notes is broken. In contrast, in Rosen if an issuer issues a value note to three different new bearers, when each of these three new notes are deposited to banks only one of the bearers will be able to receive credit for the note. As such, the Rosen system requires tamper proof devices, which are not necessary with the present invention. This is why Rosen must maintain a list of "bad money module identifiers." (See Rosen, col. 21, line 43 through col. 22, line 67, e.g.)

With regard to claims 65-68, note that Rosen's bearer's signatures are dependent on the certificates of the certification authority. If this authority issues additional bogus certificates, fake bearers could cash in on notes they previously spent. As such, the banks and the recertification authority could collude to invalidate valid notes. The present invention prevents such activity.

With regard to the Hoffman reference, the Examiner has taken the position that Hoffman's account statement 86, shown in FIG. 5 of Hoffman, reads on the electronic representation of a commodity defined in claim 73. Claim 73 defines an electronic representation of a commodity, such as monetary value, that includes first information, such as a date, up to which the electronic representation is guaranteed, and second information, such as a later date, up to which the electronic representation is valid but not guaranteed.

Applicant respectfully submits that no mention has been found in Hoffman concerning whether the monetary values in the account statement are guaranteed, not guaranteed, valid or invalid. Hoffman does indicate that the interest rate may vary from a high initial rate to a lower rate at a later time. Hoffman appears to make the amounts earned from the interest available to the customer either at designated times or at times chosen by the customer to withdraw the funds. (See col. 9, lines 22-35, e.g.) This is different from the situation where a note may have a guaranteed value at one time, and a non-guaranteed value at a later time. Consequently, Hoffman does not appear to anticipate claim 73.

Withdrawal of the rejections is requested.

Conclusion

This application is now in condition for allowance and an early action to that effect is earnestly solicited.

The Examiner is thanked for the telephone call on March 27, 2003 concerning whether a response would be filed. The Examiner is invited, and indeed encouraged, to telephone the undersigned to discuss any outstanding issues.

Respectfully submitted,

RENNER, OTTO, BOISSELLE & SKLAR, LLP

Christopher B. Jacobs

Christopher B. Jacobs, Reg. No. 37,853

1621 Euclid Avenue
Nineteenth Floor
Cleveland, Ohio 44115
(216) 621-1113

CERTIFICATE OF MAILING (37 CFR 1.8a)

I hereby certify that this paper (along with any paper referred to as being attached or enclosed) is being deposited with the United States Postal Service on the date shown below with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, U.S. Patent and Trademark Office, Washington, D.C. 20231.

March 27, 2003
Date

Christopher B. Jacobs
Christopher B. Jacobs

M:\152\DWB\DYOU\P\P0185\P0185US.R03.wpd